INTRUSION DETECTION USING A NETWORK PROCESSOR AND A PARALLEL PATTERN DETECTION ENGINE

ABSTRACT OF THE DISCLOSURE

An intrusion detection system (IDS) comprises a network processor (NP) coupled to a memory unit for storing programs and data. The NP is also coupled to one or more parallel pattern detection engines (PPDE) which provide high speed parallel detection of patterns in an input data stream. Each PPDE comprises many processing units (PUs) each designed to store intrusion signatures as a sequence of data with selected operation codes. The PUs have configuration registers for selecting modes of pattern recognition. Each PU compares a byte at each clock cycle. If a sequence of bytes from the input pattern match a stored pattern, the identification of the PU detecting the pattern is outputted with any applicable comparison data. By storing intrusion signatures in many parallel PUs, the IDS can process network data at the NP processing speed. PUs may be cascaded to increase intrusion coverage or to detect long intrusion signatures.